IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

IN THE MATTER OF THE SEARCH OF THE PREMISES KNOWN AS ROOM 53, BLDG 5, BEDFORD VETERANS QUARTERS, 204 SPRINGS RD. BEDFORD, MA, AND ANY COMPUTER OR ELECTRONIC STORAGE DEVICE FOUND THEREIN	Case No. 23-MJ-5634-JGD

AFFIDAVIT OF SPECIAL AGENT DANIEL J. MANCINI IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Daniel J. Mancini, a Special Agent with the United States Department of Veterans Affairs, Office of Inspector General, being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the United States Department of Veterans Affairs ("VA"), Office of Inspector General ("OIG"), and have been so employed since August 2017. I have been a federal law enforcement officer for approximately six years and I am currently assigned to the VA OIG Boston Resident Agency. As a Special Agent of the VA OIG, I am a federal law enforcement agent, authorized to investigate criminal offenses relating to the VA. Prior to joining VA OIG, I was employed as an Investigative Analyst with the United States Department of State, Diplomatic Security Service ("DSS") for approximately four years, where I investigated transnational criminal organizations engaged in visa and passport fraud. During my law enforcement career, I have received extensive law enforcement training. This training has included completing the Federal Law Enforcement Training Centers' ("FLETC") Criminal Investigator Training Program as well as FLETC advanced courses including Internet Investigations Training Program.

2. In addition to my training, I have experience in the investigation of various violations of federal law including mail fraud, wire fraud, false claims, child pornography, and theft of government funds, among others. Since joining the VA OIG, I have participated in a broad range of investigations as a case agent and in a subsidiary role. I have also participated in the preparation and/or execution of numerous criminal complaints, search warrants, and arrest warrants.

3. I am an investigator or law enforcement officer of the United States within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant.

4. Currently, I am the case agent in an ongoing investigation involving Timothy RYAN. During this investigation, I have worked closely with members of the Internet Crimes Against Children ("ICAC") Task Force. ICAC assigned Special Agents and Task Force Officers that have participated in this investigation have extensive training and experience investigating computer crimes and internet-related child pornography and sexual exploitation investigations. Members of the investigative team have advanced training in the area of digital evidence preservation, collection and forensic examination, and child exploitation investigations involving detecting and identifying individuals that download and share child pornography using the internet and peer-to-peer file sharing programs.

5. The facts in this affidavit are based in part on my personal observations and review of records, my training and experience, and information I learned from discussions with other law enforcement officers and witnesses. This affidavit is intended to show merely that there is probable cause for the requested search warrant and does not set forth all of my knowledge about this matter.

I have set forth only the facts that I believe are necessary to establish probable cause that evidence, fruits, and instrumentalities of the violation of Title 18, United States Code, Section 401(3), are presently located within Room #53 in Building 5 on the property of the Bedford, Massachusetts, Veterans Affairs Medical Center ("VAMC"), 204 Springs Road, Bedford, MA 01730 ("SUBJECT PREMISES").

SPECIFIED FEDERAL OFFENSES

6. *Title 18, United States Code, Section 401(3)* – A court of the United States shall have power to punish by fine or imprisonment, or both, at its discretion, such contempt of its authority, and none other, as – (3) Disobedience or resistance to its lawful writ, process, order, rule, decree, or demand.

PROBABLE CAUSE

7. My investigation began when I was contacted by the ICAC Task Force on or around November 20, 2023. According to ICAC, an IP address traced to the Bedford, MA VA Medical Center ("VAMC Bedford") was used to distribute known child pornography/child sexual abuse material ("CSAM"). The repeated distribution of CSAM activity began on or around July 4, 2023. Further analysis by the ICAC Task Force narrowed down the IP address to Building 5 at VAMC Bedford. Building 5 at VAMC Bedford is a housing program for veterans known as Bedford Veterans Quarters ("BVQ"). BVQ is located on the campus of VAMC Bedford, but is run by a private company, non-government organization Caritas Communities ("Caritas").

8. I obtained and reviewed a current roster of BVQ residents. The roster contained names of residents, dates of move in, and room numbers. The roster indicated it was updated on November 16, 2023, by "SM." I noticed there were five individuals that moved into BVQ after

the reported CSAM activity began. I did not believe these five individuals to be involved, as they moved in after the activity began.

9. I also noticed there were five individuals who moved into BVQ in the approximate month prior to when the CSAM activity began. According to the BVQ roster, RYAN moved into BVQ on or around June 26, 2023, approximately eight days before the reported CSAM activity began. I identified the five individuals, to include RYAN, via VA and law enforcement databases. Through these record checks, I learned that RYAN had an open federal case in the District of New Hampshire relating to child pornography. A lookout from the National Crime Information Center ("NCIC") indicated RYAN was on federal probation or supervised release. The miscellaneous field in the NCIC lookout indicated, "PLEASE CONTACT FEDERAL PROBATION/PRETRIAL OFFICER WITHIN 24 HOURS IF AN INQUIRY OR CONTACT IS MADE CONCERNING THIS SUBJECT TO ADVISE THE NATURE OR REASON OF THE INQUIRY OR CONTACT." The lookout also provided contact information for Probation Officer Michael Forman at the District of Massachusetts U.S. Probation Office.

10. Per the request from the NCIC lookout, I contacted U.S. Probation. While speaking with U.S. Probation personnel, I learned that RYAN was on pre-trial release/supervision out of the District of New Hampshire and was assigned to a District of Massachusetts Probation Officer because he lived at BVQ in the District of Massachusetts. Among many other conditions of release, RYAN was prohibited from using or possessing any devices that connected to the internet unless they were approved by U.S. Probation. I was advised that in RYAN's case, there were no devices approved by U.S. Probation to date.

11. On November 27, 2023, I reviewed records associated with RYAN's federal case in the District of New Hampshire. Based on the results of a separate Homeland Security

Investigations ("HSI") investigation, RYAN was charged with one count of possession of child pornography in violation of Title 18, United States Code, Section 2252A(a)(5)(B) via a complaint filed in U.S. District Court for the District of New Hampshire on December 13, 2022. I know, based on documents filed with the court as well as conversations with other law enforcement officers, that RYAN utilized an Android smartphone for the conduct referenced in the HSI investigation and open case in the District of New Hampshire.

12. According to RYAN's Order Setting Conditions of Release filed in the District of New Hampshire on January 18, 2023, RYAN was released under the following conditions, in part, depicted by the screenshots below:

IT IS ORDERED that the release of the defendant is subject to the following conditions:

☒ 1. **The defendant shall not commit any offense in violation of federal, state, or local law while on release in this case.**

☒ 8. Participate in the following computer restriction or monitoring program:

- ☒ (a) Refrain from the possession or use of a computer, electronic communication or data storage device or media, or any internet capable media device unless preapproved by the supervising officer and submit to the examination of any device owned or under the control of the defendant.
- ☒ (b) No access to the internet unless preapproved by the supervising officer.
- ☒ (c) Computer monitoring software or hardware shall be installed on defendant's computer which will be subject to periodic and unannounced examination by the supervising officer. These examinations may include retrieval and copying of data related to online use from the computer equipment and any internal or external peripheral devices. Defendant shall pay for the cost associated with the monitoring program based upon his/her ability to pay as determined by the supervising officer.
- ☒ (d) Defendant shall not access any social media websites, messaging services, and applications that have chat or messaging functions without the approval of the supervising officer (e.g., Facebook, Snapchat, Instagram, WhatsApp, Kik, etc.)
- ☒ (e) Defendant shall provide the supervising officer with all current online screen names and passwords and he/she shall not create or use any new profiles or screen names without the prior approval of the supervising officer.

☒ (f) Defendant shall notify any/all treatment programs and congregate housing programs of the above computer/internet restrictions, as set forth in 8(a)-(e). Page 3 of 5

13. The conditions of release document also advised RYAN:

TO THE DEFENDANT:

YOU ARE ADVISED OF THE FOLLOWING PENALTIES AND SANCTIONS:

A violation of any of the foregoing conditions of release may result in the immediate issuance of a warrant for your arrest, a revocation of release, an order of detention, and a prosecution for contempt of court and could result in a term of imprisonment, a fine, or both.

The commission of a federal offense while on pre-trial release will result in an additional sentence of a term of imprisonment of not more than ten years, if the offense is a felony, or a term of imprisonment of not more than one year, if the offense is a misdemeanor. This sentence shall be in addition to any other sentence.

14. RYAN signed the "Acknowledgement of the Defendant" section of this document on January 18, 2023.

15. RYAN's conditions of release were modified according to an additional Order Setting Conditions of Release document filed with the District of New Hampshire on March 17, 2023. In addition to the previous computer restriction or monitoring program set forth on January 18, 2023, RYAN was advised, "Defendant shall not use a computer, electronic or internet capable media device belonging to his roommate at VNEOC or other program." Box 11 was also checked on the new document which advised RYAN he must "Abide by all the mandatory, standard and special conditions of release as previously imposed by this court."

16. RYAN's counsel electronically signed the March 17, 2023, document "on behalf of Timothy Ryan with his permission."

17. On November 27, 2023, VA OIG Special Agents met with "E.R." and "S.M." at BVQ. E.R. is the BVQ Residential Case Manager and S.M. is the Caritas Housing Manager at BVQ. During this meeting, law enforcement agents learned that RYAN did not disclose to either E.R. or S.M. that he was restricted from accessing the internet or electronic devices.

18. On November 28, 2023, I interviewed "J.C.", a BVQ resident that lived and worked at BVQ. J.C. told me that RYAN purchased a Wavlink router from him for $30 cash shortly after RYAN moved into BVQ. J.C. brought the router up to RYAN's room and observed RYAN had a

smart television and a black Android smartphone device. J.C. said he saw RYAN with the smartphone on a daily basis and that RYAN carried the device on his person. J.C. saw RYAN with the smartphone as recently as November 27, 2023. RYAN told J.C. that the phone was not activated for cellular service or calling but it did connect to the internet via wireless connection capability.

19. On November 28, 2023, I had a teleconference with U.S. Probation personnel. U.S. Probation told me that an unannounced site visit was conducted with RYAN at BVQ earlier on this date. I learned that during the site visit, U.S. Probation personnel observed in plain view several devices capable of connecting to the internet in RYAN's room to include, a smart television, an Xbox video game console, and an internet router.

20. On November 29, 2023, RYAN appeared in federal court in Concord, New Hampshire, for a change of plea hearing before the Hon. Steven J. McAuliffe. At the conclusion of the hearing, counsel for the government advised the Court of RYAN'S apparent violations of release conditions based on the information set forth in Paragraphs 17 and 18 herein and noted concern in light of the additional information set forth in Paragraphs 7 through 9 above. The United States requested that the Court revoke RYAN's bail and remand him to the custody of the United States Marshals. The Court noted that, notwithstanding the anecdotal report by J.C. regarding his observations of RYAN with an Android cell phone, U.S. Probation did not observe any cell phones during its visit with RYAN on November 28, 2023. Nevertheless, the Court ultimately revoked RYAN's bail and remanded him to the custody of the United States Marshal.

21. On November 29, 2023, J.C. contacted VA OIG and advised that RYAN had been remanded into federal custody and would not be returning to his residence at BVQ. J.C. told VA OIG he was working at the front desk at BVQ on this date and a VA Peer Support Specialist

dropped off property that RYAN left with her as he was taken into custody by the U.S. Marshals Service. The property included a set of keys, a sweatshirt, and a wallet belonging to RYAN. Further, the VA Peer Support Specialist advised J.C. that RYAN had requested that BVQ/Caritas secure and store these items as well as the personal property located in RYAN'S room. J.C. told VA OIG that he went to Room 53, which was assigned to and occupied exclusively by RYAN, to secure RYAN's keys, sweatshirt, and wallet with his other belongings as requested. J.C. used a key—to which J.C. had access in the course of his regular duties working the front desk at BVQ—to access Room 53 to secure RYAN's property and observed in plain view a black smartphone device, an Xbox video game console, an internet router, and what he recognized as a smart television. RYAN'S belongings were left in Room 53, which was locked and secured and has remained locked and secured continuously. The keys to Room 53 are secured at the front desk of BVQ. The only persons that have access to the keys are Caritas employees.

COMPUTER DATA

22. As described in the foregoing paragraphs and in Attachment B, this application seeks permission to search for and seize any computer[1] or other internet capable and/or data storage device, as well as records and information that might be found on any such device, in whatever form they are found. One place in which the records might be found is on a computer's hard drive or other storage media. Some of these electronic records might take the form of files, documents, and other data that is user-generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis.

[1] The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

23. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for evidence that establishes how computers were used, the purpose of their use, who used them, and when.

24. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as, word processor, picture, and movie files), computer storage media can contain other forms of electronic evidence, such as, the following:

a. Forensic evidence of how computers were used, the purpose of their use, who used them, and when they were used, as described further in Attachment B, called for by this warrant. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a

residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, and correspondence (and the data associated with the foregoing, such as file creation and last accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs (and associated data) that are designed to eliminate data may be relevant to establishing the user's knowledge or intent.

CONCLUSION

25. Based on the foregoing, there is probable cause to believe that RYAN has violated 18 U.S.C. § 401(3). I therefore respectfully request that the Court issue the proposed search warrant authorizing the search of the SUBJECT PREMISES described herein and in Attachment A and the seizure of the items listed in Attachment B.

Daniel J. Mancini
Special Agent, VA OIG

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. P. 41 and affirmed under oath the contents of this affidavit and application.

Judith Gail Dein
Hon. Judith G. Dein
United States Magistrate Judge
Date: December 13, 2023

ATTACHMENT A

PREMISES TO BE SEARCHED

1. Room #53, assigned to Timothy Ryan in Building 5 (also known as the Bedford Veterans Quarters, or "BVQ") on the property of the Bedford, Massachusetts, Veterans Affairs Medical Center ("VAMC"), 204 Springs Road, Bedford, MA 01730.
2. Any computer,[2] electronic communication or data storage device[3] or media, or internet-capable media device found therein.

[2] The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

[3] The term "data storage device or media" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, compact discs, memory cards, memory chips, and other magnetic or optical media.

ATTACHMENT B

ITEMS TO BE SEIZED

The items to be seized include all information and objects that constitute fruits, evidence, and instrumentalities of violations of Title 18, United States Code, § 401(3), Contempt, including:

1. Any computer,[4] electronic communication or data storage device[5] or media, or internet-capable media device used as a means to commit the violations described above.

2. Routers, modems, and network equipment used to connect internet-capable devices to the Internet.

3. From within any computer or other internet-capable or data storage device whose seizure is otherwise authorized by this warrant (hereinafter, "DEVICE"), all records and information that relate to violations of Title 18, United States Code, § 401(3), Contempt, involving Timothy Ryan, including:

   a. All data and information revealing times the DEVICE was used or accessed;

   b. Evidence of the DEVICE'S ability to connect to a network, whether through a data plan, or a WiFi or internet connection.

   c. Evidence of who used, owned, or controlled the DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

   d. Evidence of software that would allow others to control the DEVICE, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence

[4] The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

[5] The term "data storage device or media" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, compact discs, memory cards, memory chips, and other magnetic or optical media.

of the presence or absence of security software designed to detect malicious software;

e. Evidence of the lack of such malicious software;

f. Evidence of the attachment to the DEVICE of other storage devices or similar containers for electronic evidence;

g. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the DEVICE;

h. Evidence indicating how and when the DEVICE was accessed or used to determine the chronological context of DEVICE access, use, and events relating to the crime under investigation;

i. Evidence indicating the user's knowledge and/or intent as it relates to the crime under investigation; and

j. Passwords, encryption keys, and other access devices that may be necessary to access the DEVICE.